Amendments to the Specification:

Please replace the paragraph beginning on page 1, line 2, with the following amended paragraph:

This application claims priority to U.S. Provisional Application Serial No. 60/408,856, filed September 6, 2002 ~~2003~~, the teachings of which are hereby incorporated by reference in its entirety.

Please replace the paragraph beginning on page 1, line 10, with the following amended paragraph:

In one aspect, the present invention provides an integrated firewall/VPN system that includes at least one wide area network (WAN) and at least one local area network (LAN). An integrated firewall/VPN chipset is provided that is adapted to send and receive data packets between the WAN and said LAN. The chipset includes a firewall portion configured ~~and~~ to provide access control between the WAN and the LAN and a VPN portion ~~adapted~~ configured to provide security functions for data between the LAN and the WAN. The firewall includes firewall hardware and software portions wherein at least the firewall hardware portion is ~~adapted~~ configured to provide iterative functions associated with said access control. The VPN ~~potion~~ portion includes VPN hardware and software portions wherein at least VPN hardware portion is ~~adapted~~ configured to provide iterative functions associated with the security functions.

Please replace the paragraph beginning on page 1, line 20, with the following amended paragraph:

In another aspect, the present invention provides firewall/VPN integrated circuit (IC) that ~~the~~ includes a router core ~~adapted~~ configured to interface between at least one untrusted network and at least one trusted network to send and receive data packets between the untrusted and the

trusted networks. The IC also includes a firewall system ~~adapted~~ configured to provide access control between the untrusted and trusted networks, and includes firewall hardware and software portions wherein at least said firewall hardware portion is ~~adapted~~ configured to provide iterative functions associated with access control. The IC further includes a VPN engine ~~adapted~~ configured to provide security functions for data between the untrusted and trusted networks, and includes VPN hardware and software wherein at least said VPN hardware portion is ~~adapted~~ configured to provide iterative functions associated with the security functions.

Please replace the paragraph beginning on page 4, line 21, with the following amended paragraph:

Figure 2 depicts a functional block diagram 200 of the firewall/VPN integrated system according to the present invention. The diagram 200 depicts data flow and processes for both ~~booth~~ the VPN portion and the firewall portion. Incoming data (in the form of a packet stream) 202 from the LAN or WAN is received by the network interface 204. In the exemplary embodiment, the interface 204 ~~104~~ is ~~adapted~~ configured to interface with the protocols used in the particular LAN/WAN environment, as is understood in the art. The interface 204 receives a packet stream and places the data into a packet buffer memory 206. Additionally, the system may be configured with additional and/or external memory 208 (e.g., Flash memory, SDRAM, etc.) which is ~~adapted~~ configured to temporarily store the packet data. In the exemplary embodiment, the external memory 208 is adapted to ~~top~~ store IP data packets.

Please replace the paragraph beginning on page 5, line 17, with the following amended paragraph:

The inbound VPN engine 210 generally includes decryption and decapsulation processing to convert cipher text into a plain text IP packet. As will be described more fully below with

reference to Figure 3, the VPN portion of the present invention utilizes both hardware and software to enhance the efficiency of the VPN engine. The incoming data along path 224 is placed into a conventional buffer 212. An inbound VPN processor 214 processes the data to decrypt and decapsulate the data. An inbound security associate database 216 is provided that includes a database of tunnels that associate two gateways on the WAN side, in a manner known in the art. The processor 214 uses the tunnel information in the database 216 to decrypt and decapsulate the incoming data. Also, protocol instructions 218 may be provided that includes microcodes to instruct the processor 214 to decrypt and/or decapsulate the data according to conventional and or user-defined security procedures. Once the message is decrypted and/or decapsulated, the resultant plain text (IP Packet) data is sent to the interface 204 along data path 225. In a manner described above, preselected bytes (e.g., the first 144 bytes) of the data are forwarded to the firewall 220 along path 222.

Please replace the paragraph beginning on page 6, line 22, with the following amended paragraph:

Once the data has passed the security policies, the present invention may also be ~~adapted~~ configured with quality management 242 ~~224~~ and quality of service 226 processing. The quality management processing manages the packet buffer 206 to maintain the links between queued packets stored in the memory. Quality of services 226 operates as a packet priority scheduler and will receive information from the quality of service mapping and processor 228. Essentially, and as understood in the art, quality of service analyzes the type of data coming in to determine which goes out first, based on, for example, data type (voice, IP, video, etc.) or bandwidth considerations on the network. Quality of service may also be ~~adapted~~ configured to determine the best path across the network for the data.

Please replace the paragraph beginning on page 10, line 18, with the following amended paragraph:

The Device Driver 354 provides the interface between software 302 and hardware 304. The securities policies portfolios block 356 provides the management software for the deployment of security policies. The Application tracing states table block 358 is the software component to provide detailed investigation to see which applications use the TCP/UDP/ICMP protocol. Then according to different application requirements and its stateful inspection, this software component may create associated gates in the firewall system for secure protection purpose. The Application Proxies block 360 is generally located at the Kernel level to provide more detailed investigation according to application level. This process can re-assembly the flows and contexts of in-line network traffics to make more detailed content analysis or pattern searching for the database of virus or worms, or filter unwanted commands. The Administrative software stack 362 executes the administration tasks for the system. These tasks include firewall systems and VPN engine systems. The SNMP (simple ~~small~~ network management protocol) stack 364 is provided to execute the SNMP according to general RFC requirement. This component is the interface for the general network device or network software stack to get the status or any statistics or logs in the system.

Please replace the paragraph beginning on page 11, line 20, with the following amended paragraph:

The Administrative Web Browser Management provides Web based management GUI (graphic user interface) component. In the exemplary system, the system general CPU will host web server under HTTPS protocol, the management web page will be stored in this web server. All configuration and management process for the system can be collaborated within this page point. By using socket layer SSL (Secure Sockets Layer), the management web page can be browsed remotely (in WAN host), or local secure LAN host with the encrypted connection.(i.e.

the connection uses the chosen encryption algorithm to provide high degree privacy). The Local CLI(command line interface)/Tiny File System(TFS) 374 is adapted to provide local access with command line and configuration files interaction.

Please replace the paragraph beginning on page 15, line 16, with the following amended paragraph:

In this VPN engine, an array of micro-coded microprocessors ~~uPs~~ are the foundation to provide the flexibility of different security protocols (in addition to Ipsec). The microprocessors include programmable instruction memory to permit updates of multi-protocol functions.